CLAIMS

1. An integrated circuit comprising a processor and non-volatile memory, the non-volatile memory storing a first number and a second number, wherein the second number is the result of an encryption function taking a third number and secret information as operands, the integrated circuit comprising software configured to decrypt the second number using the first number, thereby to determine the secret information as required.

2. An integrated circuit according to claim 1, wherein the first and third numbers are the same.

3. An integrated circuit according to claim 1, wherein the first and second numbers are of the same length.

4. An integrated number according to claim 1, wherein the first number is a random number that was generated using a stochastic process.

5. An integrated circuit according to claim 1, wherein the encryption function is an XOR logical function.

6. An integrated circuit according to claim 5, wherein the software is configured to decrypt the second number by performing an XOR logical function using the first and second numbers as operands.

7. A method of manufacturing a plurality of integrated circuits in accordance with claim 1, including the steps, for each integrated circuit, of:

determining the first number, the third number and the secret information;

generating the second number by way of an encryption function that uses the third number and the secret information as operands;

storing the first and second numbers on the integrated circuit.

8. A method according to claim 7, wherein the first number is different amongst at least a plurality of the integrated circuits.

9. A method according to claim 8, wherein the first numbers are determined randomly, pseudo-randomly, or arbitrarily.

10. A method according to claim 7, wherein the first number is stored on the integrated circuit first, then extracted therefrom for use in generating the third and thence the second number.